ABSTRACT

Various methods and apparatuses are provided for generating and verifying digital signatures. In certain methods and apparatuses digital signature generating logic encrypts data based on a Jacobian of a curve, said Jacobian having a genus greater than one. The logic is configured by parameter data so as to select at least one Gap Diffie-Hellman (GDH) group of elements relating to the curve. The logic also determines private key data and corresponding public key data and signs the identified data with the private key data to create a corresponding digital signature. In other methods and apparatuses, the signature generating logic encrypts data based on a Weil pairing on a Jacobian of at least one super-singular curve having a genus greater than one.